WORTHING COLLEGE STUDENT

IT SECURITY POLICY

MAY 2018

Policy name	Student Information Technology Security Policy
Author:	Michael Perry
Approved by SMT	May 2018
Approved by Corporation	Not required
Date for next review:	May 2019

Through its policies and in its day to day work, the College is committed to promoting equality and fairness and combating discrimination. This applies to everyone, regardless of gender, racial or ethnic background, disability, religion, sexual orientation or age and embraces the College's legal responsibilities.

WORTHING COLLEGE

STUDENT INFORMATION TECHNOLOGY SECURITY POLICY

College mission
The Mission of Worthing College is to provide: Opportunity, Achievement, Success and Progression

Mission

To inspire, build confidence and prepare you for the life you want to live.

Vision

"We'll believe in you"

Whatever your background, identity or experience of learning to date, we believe in you. We will support your achievement and success.

"We'll take you further than you expect"

You'll have the opportunity to choose from the widest possible range of courses in one place and we'll stop at nothing to connect you with the best university, employer, or apprenticeship for you. And if you're already working, we'll help you to keep developing and growing.

"We'll provide an inspirational environment for you"

You'll experience a warm welcome from our community. You'll grow in confidence, resilience and be ready for progression to the next step in your life, whether that's further study, the world of work or your own unique adventure.

Values

"For us to succeed in our mission and vision, the College has shared community values which help pull us together to act in agreed ways as part of an inspirational community."

"We listen intently to the voice of those we serve and show unending commitment to continuous improvement and innovation."

"We engage fully with the needs of the local community, employers and universities so we can secure your achievement, success and progression."

"We respond quickly, so we're always able to give you the best support, information, advice and guidance, just when you need it."

"We celebrate together the successes and diversity of our community."

Aim of the policy

- To set out the College's commitment to provide students with the IT facilities they need for their work and to outline the acceptable and unacceptable use of all IT systems
- To inform students of the levels of monitoring carried out by the College
- Outline the consequences of not abiding to this policy
- Provide recommendations for good practice.

Other related policies

- Communications policy
- Student disciplinary policy
- Data Protection policy
- Harassment policy
- College values and beliefs

Legal framework

Many aspects of IT use in College are governed by regulation and the College is required by law to comply with these. The following acts particularly apply to IT use and security

- Computer Misuse Act 1990
- Data Protection Act 2018
- Malicious Communications Act 1988
- Regulation of Investigatory Powers Act 2000
- Copyright act 1988

There are a number of other Acts of Parliament which apply to computer systems and networks. In particular, the Computer Misuse Act makes it illegal to

- Gain unauthorised access to a computer's software or data - including the illegal copying of programs.
- Gain unauthorised access to a computer's data for illegal purposes.
- Gain unauthorised access to a computer's data with the intention of altering or deleting it
- Copy programs illegally

A conviction may lead to a fine and a 5-year prison sentence.

College commitment to information technology

- The College is committed to providing all students with access to the necessary IT facilities and support to enable them to undertake their studies at the College effectively. This includes use of computers, printers and other facilities associated with them, e.g. access to the network, software, email, the Internet, Intranets (Moodle) etc.
- The college will provide wireless access in certain areas for students to use their own portable devices (such as laptops, smartphones etc.) in support of their studies.

- The College is committed to exploring the use of emerging technologies to enable better internal and external communication, to gain access to information and to support learning.
- The IT Services Support team will be available to offer support and guidance on how to use the College network and resolve difficulties. They can be found in Room G58 or by email at itservicesteam@worthing.ac.uk

Consequence of misuse
Any student suspected of computer misuse may have their user accounts suspended and this may be treated by the College as a serious disciplinary offence. Serious misuse may lead to disciplinary action under the student Disciplinary Policy being taken or being asked to leave the college. Depending on the severity of misuse, students may also be liable for prosecution in line with current legislation.

1. User accounts and passwords
The College will issue each student with a College network username and password at induction. Students must agree to abide by the IT security policy which is available on the student intranet under policies and on the college website.

Usernames and passwords should not be divulged to anyone. If misuse occurs, the College will assume that a student has not complied with this policy unless they have substantial evidence to prove that someone else has misused their details.

Student passwords must be:
- At least 8 characters long.
- Changed at least once every year
- Different to the last 3 passwords used.

Acceptable use:
- Students are entrusted with individual network credentials that consist of a username and password, which should remain private.
- Students should use their individual username and password to gain access to the computer facilities and services provided by the College for legitimate educational and private/recreational purposes only.
- To transfer documents between a College email account and an external email account for legitimate educational or College purposes. Documents transmitted in this way are subject to security risks and should not contain data that may identify individuals.

Unacceptable use: Students should not
- Divulge their username and password to anyone else.
- Allow another student to use their username and password either willingly or unwillingly.
- Use another student's username and password with or without their consent.
- Use their or anyone else's network credentials to access the College computer facilities for business purposes or for accessing content of an inappropriate nature.
- Leaving a computer for any period of time when they are still "logged on".

Best practice tips:
- Log off or lock a PC if you have to leave the room – regardless of how long you are likely to be away.
- Change your password regularly – you will be periodically prompted to do so by the network.
- Never write your username and password down or store it electronically.

2. Use of email
The College will issue each student with an individual email address. This address is intended to be used for College related matters. A record of all email activity will be kept for a period of one month.

Any personal information about another individual, transmitted by email, is subject to the Data Protection Act. This includes names, addresses, phone numbers and email addresses. It is important to ensure that such information is accurate and is used only for the purpose for which it was collected.

The status of an email is the same in law as any other written communication. Care should, therefore, be taken that no information or opinion is transmitted about another individual that is unfounded, inaccurate or defamatory. In extreme cases, this may lead to legal action and a student being asked to leave the

college.

The College cannot guarantee the confidentiality of information transmitted via email. If in doubt, use another method. Keep in mind that the College owns any communication sent via email or that is stored on College equipment. The College has the right to access any material in a student's email or computer at any time. Students should not consider electronic communication, storage or access to be private if it is created or stored at college.

Emails sent outside the College using the College email system will display the College's standard disclaimer.

Acceptable use:

- Communication with others (both within the College and externally) on matters relating to College work and activities.
- Limited personal use as long as it does not interfere with work. This must, however, be kept to a minimum.
- To send documents between the College and an external email account for access away from the College such as at home.

Unacceptable use:

- Using inappropriate, insulting, or offensive language or material
- Creating or transmitting any materials that may be construed by the recipient as being offensive, obscene, pornographic, indecent, abusive, defamatory, slanderous, harassing or threatening, that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, and marital status, and disability, political or religious beliefs.
- Adversely commenting on integrity, personality, honesty, character, intelligence, methods or motives of another person unless it is a factual response to a formal reference request.
- Transmitting junk mail of any kind, to any other students or organisations that is designed or likely to cause annoyance, inconvenience or needless anxiety.
- Transmitting material such that this infringes the copyright of another person, including intellectual property rights.
- Activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other staff or students.
- Creating or transmitting material that corrupts or destroys other students' data or violates the privacy of other students.
- Creating or transmitting material that includes false claims of a deceptive nature.
- Creating or transmitting material that brings the College into disrepute.
- Transmitting by email any file attachments that they know to be infected with a virus.
- Opening email file attachments received from non-trusted sources.
- Using email for commercial or profit-making activities or for any other form of personal financial gain – especially gambling and unsolicited advertising.
- Publishing to others the text of messages written on a one-to-one basis, without the prior express consent of the author.

Best practice tips:

- Send emails only to people that you know.
- If the College blocks the transmission of an email and feels there is a legitimate reason for the transmission to be completed, contact the IT Services team who will consider each individual case.
- If you worried about whether the content of an email is inappropriate, contact the IT Services team for guidance.
- Check your inbox regularly.
- Delete unnecessary emails regularly to prevent over-burdening the system.
- Think before you write. Do not make statements which you would not be prepared to repeat publicly
- Keep messages as brief and to the point as possible
- Avoid the use of upper case, different colours or large fonts as these can appear aggressive.

3. Internet use

The College provides Internet access from all student computers. This access is intended for educational use only, with limited personal use.

Acceptable use:

- To access resources relating to teaching and learning to help you complete your course.
- Excessive personal use may be regarded as a disciplinary matter.

Unacceptable use:

- Creating, transmitting, accessing or downloading (other than for properly supervised and lawful research purposes) any materials that may be construed as being offensive, obscene, pornographic, indecent, abusive, harassing or threatening.
- Creating, transmitting, accessing or downloading material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- Accessing, playing and downloading games.
- Downloading and installing any applications, programs or executable files which may introduce malicious software into the College network
- Creating or transmitting defamatory material.
- Transmitting material such that this infringes the copyright of another person, including intellectual property rights.
- Using the Internet for commercial or profit-making activities or for any other form of personal financial gain – especially gambling and unsolicited advertising.

Best practice tips:

- If you are worried about whether the content you wish to view is inappropriate, please contact the IT Services team for guidance.
- If the College blocks access to a resources on the Internet and you feel there is a legitimate reason for access to be allowed, contact the IT Services team who will consider each individual request.

The college promotes the government's Prevent strategy to prevent radicalisation of young people. As part of this we will take steps to ensure that access to extremist websites of a political, religious or social nature is blocked.

4. Data storage

Data should be stored in the following network locations:

- OneDrive

My Documents

Acceptable use:

- Storing data that is current and relevant to the courses you are studying at College.

Unacceptable use:

- Storing large amounts of data of a personal, non-College related nature.
- Retaining data which is inaccurate or obsolete.

Best practice tips:

- Regularly review your documents and delete those which are no longer required. Documents can be copied to removable media if required: - contact the IT Services Team for assistance.

5. Data backup

The College will make daily backups of all key College data held on College servers and store this off site in a secure location The College will retain backup copies of all data for six months and email for one month. Students may also wish to ensure that their documents are backed up to external devices. Documents stored on local PCs in student areas are not backed up. The use of portable computers and laptops to create and store documents also creates a risk of lost data.

Best practice tips:

- When using College PCs, store documents in the 'My Documents' folder or OneDrive
- Avoid storing documents on local drives on College PCs
- If documents are created on laptops or other portable devices, back these documents up to the College network. Please refer to the IT Services team if you need any assistance

6. Use of software
All software must be properly licensed and should be evaluated by the IT Services team prior to installation to ensure compatibility with the College network. Software should only be installed by the IT Services team. The IT Services team will maintain an inventory of all software installed on the College network. Use of licensed software without a licence or use of software outside the terms of the licence is illegal and may be treated as a disciplinary offence

Acceptable use:
- Students can use any software that has been loaded onto the computers they are accessing provided they are sure this software has been installed by the IT Services team.

Unacceptable use: Students should not
- Download or install any software from the Internet without reference to the IT Services team
- Install unlicensed copyrighted software on to the College network
- Use software when they are unsure of the legitimacy of the licence.
- Duplicate any licensed software on the College network

Best practice tips:
- If you are in any doubt about the legitimacy of the software installed on your PC or the College network, please contact the IT Services team for guidance.

7. Network monitoring
By law, the College is able to monitor the use of computers by students. The College will monitor all electronic communication and Internet activity. The monitoring will include:
- Scanning all data for viruses.
- Scanning all emails to detect and remove unsolicited (spam) emails.
- Scanning of all Internet access to ensure all traffic is of a legitimate nature.
- Maintaining audit logs of unsuccessful attempts to log on to the network.
- Maintain audit logs of websites students have visited.

The network administrators will be granted access to all information stored on the network.

The College will implement solutions to try to ensure control of the following threats:
- Computer viruses – anti-virus software is installed on all PCs to try to eradicate the threat of infection.
- Unauthorised Internet access – Internet site access is filtered to prevent access to inappropriate material.
- Identity theft (phishing) - anti-phishing software is installed on all PCs to try to eradicate the threat of infection.
- Unsolicited email (spam) – incoming email is filtered to intercept spam emails.

Best practice tips:
- Do not open suspect emails or Internet links. Do not reply to such emails and never divulge any personal details online.
- Reduce the risk of phishing - phishing is a type of deception designed to steal your valuable personal data such as credit card numbers, and other account data and passwords. Phishing is also known as identity theft. This often appears as a spoof of well-known businesses web sites e.g. banks, requesting your account access details. You may also receive message that you have won or inherited a large amount of money or even that your computer is unsafe and you need to run special software scans. As with email spam, do not reply to such emails and never divulge personal details online.
- If you are in any doubt about the authenticity or appropriateness of the email/website, please seek guidance from the IT Services team.
- If you feel certain communications are being blocked and this is inhibiting your ability to work productively, please report the issue to the IT Services team who will consider your request.

8. Electronic connectivity
The College will provide the following facilities for electronic communications between the College and the outside world:
- Internet connectivity to allow students to upload data to external websites.
- Web based access of the Student Intranet to enable students to access details of their courses from

outside the college or with their own mobile device (laptop, smartphone etc.).
- Web based access to a student's college email account.

Best practice tips:
- Please refer to the IT Services team if you need any clarification as to whether a certain activity is permitted or not.

9. Portable computing devices including devices provided by the college
Portable devices that carry data include laptops, USB data sticks, external drives, flash memory devices, mobile phones, tablets, smart phones and iPods etc. These devices have the capacity to hold large amounts of data. If a student takes inappropriate data outside of the college, they may be breaching the terms of the Data Protection Act.

Best practice tips:
- Devices should use a password where possible.
- Devices should not be used to transport personal or confidential data out of the building
- Devices should store data in an encrypted format
- Devices should be physically secure if possible i.e. kept in a locker
- Device should not be left unattended. Students should take all safeguards possible to avoid unauthorised access to these devices.
- In the event of theft of devices containing sensitive data, this must be reported to IT Services immediately

10. Access to information
The College reserves the right to control access to information and systems in line with the Data Protection Act to preserve confidentiality and to protect students from exposure to data that they are not entitled to access.

The College will grant students access to resources that are appropriate to their responsibilities within the organisation. The College will also grant access to information that students are legally entitled to view.

Students should not divulge information relating to the College or any individual attending the College to third parties without reference to the IT Services team for guidance.

Acceptable use:
- Accessing information that relates to you or that you need for your courses.

Unacceptable use:
- Trying to obtain access to information that you have no legitimate business purpose to view.
- Disclosing personal information about anyone to a third party without either the express consent of the individual that the data refers to or without seeking guidance from the IT Services team

Best practice tips:
- Any requests from a third party for information or data regarding the College or any of its employees or students should be referred to the IT Services team before any information is divulged.

11. Use of Social Networking Sites
Students are reminded of their commitments that the college has set out in its Values, Beliefs and Behaviours. This means that a student should not use social networking sites to criticise or be negative about the work of the college, its staff or other students. They are reminded that the college has a complaints policy which should be used if they have concerns about the work of the college.

Any student who is deemed to violate any of these policies and principles will be subject to the college's disciplinary procedures and may jeopardise their place at the college.

The college acknowledges that the use of social networking sites such as Facebook, Snapchat, Instagram and Twitter etc. are a fast growing phenomenon. The College will support students in getting the most out of these sites while at the same time controlling any abuse of such sites that negatively impacts on teaching and learning, the college's security or reputation and the safety and security of staff and students.

- Students are advised on the safe use of IT through the tutorial programme. The college supports the advice and guidance offered by the UK Council for Child Internet Safety's Click Clever, Click

Safe campaign as follows -

- When you're online, always keep your personal information private and think about what you say and do.
- Remember that people online may not be who they say they are. Online friends are still strangers even if you have been talking to them for a long time.
- Don't share personal information online. This includes your full name, photos, addresses, school information, telephone numbers and places you like to spend time.
- Make sure you have set your privacy settings to restrict access to personal information.
- When you use chat rooms or instant messenger, use a nickname instead of your real name.
- To stop people accessing your online accounts, always keep your passwords secret and change them regularly.
- Think about blocking people who send you unpleasant messages and don't open unknown links and attachments.
- Always delete emails from people you don't know, and don't open attachments from people you don't know. They might be unpleasant or contain a virus that can stop your computer working.
- If someone sends you unpleasant or threatening messages online, block them.
- If you see anything that upsets you online or if someone asks to meet you, flag it up with someone you trust.
- If you are worried or unhappy about anything you see online, tell your tutor. If a friend you have made online asks to meet you in person, talk to your parents or your tutor about it. You should never meet up with someone you have met online because it is dangerous.
- If someone you know is being unpleasant to someone online, speak to your tutor about it.

In addition, all students are advised to consider the advice from www.bullying.co.uk, which provides detailed guidance on protecting yourself from cyberbullying and harassment below. However, if you are subjected to any form of cyberbullying or harassment or know of another student who is, please report this to your tutor in the first instance, or Student Advice and Support.

If you are a victim of cyber bullying

- Leave the area or stop the activity (i.e. chat room, online game, instant messaging, social networking site, etc.).
- Block the sender's messages.
- Never reply to harassing messages.
- Talk to your tutor. If the bullying includes physical threats, the police may need to be informed as well.
- Save any harassing messages and forward them to your tutor.

The college promotes the government's Prevent strategy to prevent radicalisation of young people. As part of this we will take steps to ensure that access to extremist websites of a political, religious or social nature is blocked.

Declaration

A full copy of this policy will be displayed in all IT classrooms and is available on the student intranet and the college website.